(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 379 029 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
30.08.2006 Bulletin 2006/35

(51) Int Cl.:
H04L 12/28 *(2006.01)*

(21) Application number: **03254269.8**

(22) Date of filing: **04.07.2003**

(54) **Method of guaranteeing users' anonymity and wireless local area network (LAN) system therefor**

Verfahren zum Garantieren der Anonymität von Benutzern sowie Drahtloses lokales Netzwerksystem (LAN)

Méthode pour garantir l'anonymat des utilisateurs et réseau local sans fil correspondant

(84) Designated Contracting States:
DE FR GB

(30) Priority: **06.07.2002 KR 2002039155**

(43) Date of publication of application:
07.01.2004 Bulletin 2004/02

(73) Proprietor: **SAMSUNG ELECTRONICS CO., LTD.**
Suwon-City, Kyungki-do (KR)

(72) Inventors:
- **Jang, Kyung-hun**
  Paldal-gu,
  Suwon-city,
  Kyungki-do (KR)
- **Park, Jong-ae,502-705 Jinsan Maeul Samsung 5cha ap**
  Yongin-city,
  Kyungki-do (KR)
- **Lee, In-sun**
  Yongsan-gu,
  Seoul (KR)

(74) Representative: **Greene, Simon Kenneth**
Elkington and Fife LLP,
Prospect House,
8 Pembroke Road
Sevenoaks,
Kent TN13 1XR (GB)

(56) References cited:
WO-A-01/19053
WO-A-01/43466
WO-A-97/48246
WO-A-99/37103
US-B1- 6 256 300

- **GUPTA V ET AL: "The design and deployment of a mobility supporting network" PARALLEL ARCHITECTURES, ALGORITHMS, AND NETWORKS, 1996. PROCEEDINGS., SECOND INTERNATIONAL SYMPOSIUM ON BEIJING, CHINA 12-14 JUNE 1996, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, US, 12 June 1996 (1996-06-12), pages 228-234, XP010166783 ISBN: 0-8186-7460-1**

EP 1 379 029 B1

Description

[0001] The present invention relates to wireless Local Area Network (LAN) system. More particularly, the present invention relates to a method of guaranteeing a user's anonymity and a wireless LAN system therefor, by using a temporary address generated from a unique Media Access Control (MAC) address as a source address or a destination address.

[0002] Generally, a wireless LAN system consists of an ad-Hoc network where a plurality of terminals, each of which includes a wireless Network Interface Card (NIC), are connected to each other and independently to wired LANs, and an infrastructure network where wireless terminals are connected to wired LANs through wireless access nodes. In an infrastructure network, a wireless cell Basic Service Set (BSS) is formed centering on one wireless access node. The wireless access node has the same functionality as a cellular phone station and connects all wireless terminals in the BSS to a LAN.

[0003] FIG. 1 illustrates a conceptual scheme showing the structure of a wireless LAN system of a general infrastructure network. A wireless LAN system as shown in FIG. 1 consists of a wireless access node 11 and four wireless terminals 13, 15, 17, and 19. The wireless access node 11 is connected to a wired network, such as very-high-speed Internet lines or private lines, and performs access arbitration between wireless terminals. The four wireless terminals 13, 15, 17, and 19 form a BSS and include wireless LAN cards respectively. The wireless LAN cards installed respectively in the first to fourth wireless terminals 13, 15, 17, and 19 have MAC addresses MAC Addr1 to MAC Addr4 corresponding to the first to fourth wireless terminals 13, 15, 17, and 19.

[0004] The unique MAC addresses MAC Addr1 to MAC Addr4 allocated to the respective wireless LAN cards of the first to fourth wireless terminals 13, 15, 17, and 19 are used as source addresses or destination addresses when sending and receiving data packets between the first through fourth wireless terminals 13, 15, 17, and 19 through the wireless access node 11. That is, to transmit a data packet (for example, a protocol data unit (PDU)) to one wireless terminal among the first to fourth wireless terminals 13, 15, 17, and 19, the wireless access node 11 sends transmission frames 12, 14, 16, and 18, each of which contains a unique MAC address (i.e., a MAC address among the first to fourth MAC addresses MAC Addr1 to MAC Addr4) of a wireless terminal representing the destination address. The address is placed in the header of the data packet (PDU) to be transmitted. On the other hand, each of the first to fourth wireless terminals 13, 15, 17, and 19 compares the MAC address corresponding thereto with the destination addresses contained in the headers of the transmission frames 12, 14, 16, and 18 sent from the wireless access node 11. If a destination address is identical to the MAC address corresponding to a wireless terminal, the corresponding wireless terminal accepts the frame. If no match is made, the frame is dropped over the network.

[0005] MAC addresses used for data communication between wireless terminals through wireless access nodes are unique values allocated upon manufacturing wireless LAN cards. The MAC address is not varied and also not encoded. Accordingly, MAC addresses are exposed during data communication so that anonymity of a user using a corresponding MAC address can not be guaranteed. Thus, a user using the corresponding MAC address may be easily tracked. That is, by merely monitoring unique MAC addresses, private user information about network access state, network access time, etc., may be outflowed, and more seriously, if any unique MAC address is exposed, a greater risk exists for malicious users eavesdropping at the link layer. Further, attack possibility to encryption channels is increased in long-running monitoring.

[0006] As described above, since it is necessary to guarantee a user's anonymity so that information about a user of a wireless LAN system is not leaked to objects other than a permitted entity, the conventional wireless LAN system of the infrastructure network has many security problems.

[0007] According to a feature of an embodiment of the present invention, there is provided a method of guaranteeing users' anonymity in a wireless LAN system, the method comprising: (a) creating a plurality of temporary address sets, each of which corresponds to a unique Media Access Control (MAC) address of a wireless terminal, and transmitting each temporary address set to the corresponding wireless terminal, and (b) performing data packet transmissions between a wireless terminal and a wireless access node using a temporary address selected from the temporary address set corresponding to the wireless terminal as a source address or a destination address.

[0008] In the method above, the wireless access node may create the temporary address sets, each of which preferably consists of N (where N is an integer greater than or equal to two) temporary addresses using a MAC address contained in an access or authentication request message transmitted from a corresponding wireless terminal.

[0009] In the method above, in (a), the wireless access node may encode the temporary address sets using a predetermined encryption key for each temporary address set, and may respectively transmit the encoded temporary address sets to the corresponding wireless terminals. Each encryption key may be created upon authentication of the corresponding wireless terminal.

[0010] In the method above, (b) may further include (b1) a first addressing, which is performed in the wireless access node, and generates a temporary address as a destination address randomly selected from the temporary address set corresponding to a wireless terminal that is requesting authentication. Also, (b) may include (b2) a second addressing,

which is performed in the wireless terminal, and generates a temporary address as a source address randomly selected from the temporary address set corresponding to the wireless terminal.

[0011] According to another feature of an embodiment of the present invention, there is provided a computer readable medium having embodied thereon a computer program for performing the method described above.

[0012] According to another feature of an embodiment of the present invention, there is provided a wireless Local Area Network (LAN) system for guaranteeing users' anonymity comprising: a wireless access node arranged to create a plurality of temporary address sets, each of which corresponds to a unique Media Access Control (MAC) address of a wireless terminal, and use a temporary address selected from each temporary address set as a destination address; and at least one wireless terminal arranged to receive a temporary address set corresponding to a unique Media Access Control address thereof from among the plurality of temporary address sets created in the wireless access node, and use a temporary address selected from the received temporary address set as a source address.

[0013] In the system above, the wireless access node may create the temporary address sets, each of which consists of N (where N is an integer greater than or equal to two) temporary addresses, preferably using for each address set the MAC address contained in an access or authentication request message transmitted from the corresponding wireless terminal.

[0014] In the system above, the wireless access node preferably encodes the temporary address sets using a predetermined encryption key for each address set, and respectively transmits the encoded temporary address sets to the corresponding wireless terminals. Preferably, each encryption key is created upon authentication of the corresponding wireless terminal.

[0015] In the system above, the wireless access node may include a first memory, which stores the plurality of temporary address sets, each of which consists of N (where N is an integer greater than or equal to two) random addresses and is created corresponding to a unique MAC address, a first MAC address filter, which filters a unique MAC address from a source address of a data packet received from a corresponding wireless terminal by referring to the temporary address sets stored in the first memory, a destination address generation unit, which enables a temporary address set corresponding to the unique MAC address of the wireless terminal requesting authentication from among the temporary address sets stored in the first memory, generates a first random selection signal, generates a temporary address randomly selected from the enabled temporary address set, and uses the temporary address as a destination address, and a first random selection unit which randomly selects a temporary address from the temporary address set enabled in the first memory according to the first random selection signal generated in the destination address generation unit, and outputs the selected temporary address to the destination address generation unit.

[0016] The wireless terminal may include a second memory which receives a temporary address set from the wireless access node and stores the temporary address set corresponding to a unique MAC address of the wireless terminal, a second MAC address filter which determines whether a destination address of a data packet received from the wireless access node is included in the temporary address set by referring to the temporary address set stored in the second memory, and generates a receipt enable signal according to a determination result, a source address generation unit, which generates a second random selection signal according to a source address request signal, generates a temporary address randomly selected from the temporary address set stored in the second memory, and uses the temporary address as a source address, and a second random selection unit which randomly selects a temporary address from the temporary address set stored in the second memory according to the second random selection signal generated in the source address generation unit, and outputs the selected temporary address to the source address generation unit.

[0017] The present invention thus provides a method for guaranteeing a user's anonymity in a wireless Local Area Network (LAN) system by using a temporary address randomly selected from a temporary address set that contains mapping to a Media Access Control (MAC) address as the source address or the destination address upon transmitting data packets between a wireless access node and wireless terminals.

[0018] The present invention further provides a wireless LAN system for guaranteeing a user's anonymity by using a temporary address generated from a unique MAC address.

[0019] The above and other features and advantages of the present invention will become more apparent to those of ordinary skill in the art by describing in detail preferred embodiments thereof with reference to the attached drawings in which:

FIG. 1 illustrates a conceptual scheme showing the structure of a general wireless Local Area Network (LAN) system;

FIG. 2 is a flow chart for describing a method of guaranteeing users' anonymity in a wireless LAN system according to a preferred embodiment of the present invention;

FIG. 3 illustrates a view for describing an operation relationship between a wireless access node and wireless terminals;

FIG. 4 is a block diagram showing a detailed structure of an addressing unit of the wireless access node in the wireless LAN system according to a preferred embodiment of the present invention; and

FIG. 5 is a block diagram showing a detailed structure of an addressing unit of the wireless terminal in the wireless

LAN system according to a preferred embodiment of the present invention.

[0020] FIG. 2 is a flow chart for describing a method of guaranteeing users' anonymity in a wireless LAN system according to an embodiment of the present invention. The method of guaranteeing users' anonymity includes access step 21, authentication step 22, temporary address set generation step 23, temporary address set transmission step 24, and data packet transmission step 25. FIG. 3 illustrates a view for describing the operation relationship between a wireless access node and wireless terminals. Signal transmissions between a wireless access node and a wireless terminal in the above-mentioned steps are illustrated in FIG. 3.

[0021] Now, the steps shown in FIG. 2 will be described in connection with FIGS. 1 and 3.

[0022] In the access step 21, if a first wireless terminal 13 requests access, access between the first wireless terminal 13 and a wireless access node 11 is performed. For performing this access, the first wireless terminal 13 transmits to the wireless access node 11 an access request message Association_Req containing its own unique MAC address MAC Addr1 as the source address (process 31 of FIG. 3). The wireless access node 11, which receives the access request message Association_Req, tries to access the first wireless terminal 13. If this access succeeds, the wireless access node 11 transmits to the first wireless terminal 13 an access success message Association_Resp containing the unique MAC address MAC Addr1 of the first wireless terminal 13 as the destination address (process 32 of FIG. 3).

[0023] In the authentication step 22, if a first wireless terminal 13 requests authentication, the wireless access node 11 performs authentication of the first wireless terminal 13. For performing this authentication, the first wireless terminal 13 transmits to the wireless access node 11 an authentication request message Authentication_Req containing its own unique MAC address MAC Addr1 as the source address (process 33 of FIG. 3). The wireless access node 11, which receives the authentication request message Authentication_Req, performs an authentication of the first wireless terminal 13. If the authentication succeeds, the wireless access node 11 creates an encryption key. At this time, the wireless access node 11 transmits to the first wireless terminal 13 the encryption key in the authentication success message Authentication_Resp containing the unique MAC address MAC Addr1 of the first wireless terminal 13 as the destination address (process 34 of FIG. 3).

[0024] In the temporary address set generation step 23, the wireless access node 11 randomly transforms the unique MAC address MAC Addr1 of the first wireless terminal 13 contained in the authentication request message Authentication_Req, and creates a temporary address set consisting of N temporary addresses corresponding to the unique MAC address, wherein N is preferably an integer greater than or equal to two (process 35 of FIG. 3).

[0025] In the temporary address set transmission step 24, the temporary address set created in the wireless access node 11 is encoded using the encryption key created in the authentication step 22, and then is transmitted to the first wireless terminal 13 using the unique MAC address MAC Addr1 of the first wireless terminal 13 as the destination address (process 36 of FIG. 3).

[0026] In the data packet transmission step 25, whenever data communication is performed between a first wireless terminal 13 and wireless access node 11, a temporary address is randomly selected from a temporary address set and assigned to the data packet as a source address or destination address. That is, when the first wireless terminal 13, which receives an authentication success message Authentication_Resp and a temporary address set from the wireless access node 11, tries to transmit a data packet PDU to the wireless access node 11, the first wireless terminal 13 addresses as the source address a temporary address, i.e., a first temporary address Taddr1, randomly selected from the N temporary addresses in the temporary address set and transmits the data packet PDU (process 37 of FIG. 3). On the other hand, when a data packet PDU is transmitted from the wireless access node 11 to the first wireless terminal 13, a temporary address, i.e., a third temporary address Taddr3, randomly selected from the N temporary addresses in the temporary address set, is set as the destination address and the data packet PDU is transmitted (process 38 of FIG. 3).

[0027] FIG. 4 is a block diagram showing a detailed structure of an addressing unit 40 of the wireless access node 11 in the wireless LAN system of the present invention. The addressing unit 40 includes a memory 41, a MAC address filter 43, a destination address generation unit 45, and a random selection unit 47, for addressing the destination addresses used in the data packet transmission step (step 25) described with reference to FIG. 3.

[0028] Referring to FIG. 4 in addition to FIGS. 1-3, operations of the addressing unit 40 will now be described. After a wireless access node 11 completes authentication of a first wireless terminal 13, a temporary address set which consists of N temporary addresses randomly created corresponding to a unique MAC address of the first wireless terminal 13, are stored in memory 41. At this time, a temporary address set is created corresponding to a unique MAC address for each wireless terminal requesting authentication and the temporary address sets are stored in the form of a look up table in memory 41.

[0029] A MAC address filter 43 works together with memory 41 when a data packet is transmitted from the first wireless terminal 13 to the wireless access node 11. The destination address generation unit 45 and the random selection unit 47 work together with memory 41 when a data packet is transmitted from the wireless access node 11 to the first wireless terminal 13. Operations of these components will be described in detail as follows.

[0030] The MAC address filter 43 receives a source address (SA) extracted from the data packet transmitted from the

first wireless terminal 13, and attempts to discover a temporary address set including a temporary address matching the source address by referring to the plurality of temporary address sets stored in memory 41. If the temporary address set is found, a unique MAC address corresponding to the temporary address set is extracted and transmitted to any layers requiring it.

[0031] The destination address generation unit 45 receives the unique MAC address of the first wireless terminal 13 obtained in the access/authentication steps, finds a temporary address set corresponding to the received unique MAC address among the plurality of temporary address sets stored in memory 41, activates the found temporary address set, and then outputs a random selection signal to a random selection unit 47.

[0032] The random selection unit 47 randomly selects a temporary address from the temporary address set activated in memory 41, depending on the random selection signal, and outputs the selected temporary address to the destination address generation unit 45. The destination address generation unit 45 sets the temporary address received from the random selection unit 47 as the destination address (DA), and outputs the destination address (DA).

[0033] That is, whenever data packets are transmitted from the wireless access node 11 to the first wireless terminal 13, each data packet has a different destination address from the others. This applies equally to other wireless terminals in a BSS (Basic Service Set).

[0034] FIG. 5 illustrates a block diagram showing a detailed structure of an addressing unit 50 of the first wireless terminal 13 in the wireless LAN system according to the present invention. The addressing unit 50 includes a memory 51, a MAC address filter 53, a source address generation unit 55, and a random selection unit 57, for addressing the source addresses used in the data packet transmission step 25 described with reference to FIG. 3.

[0035] Referring to FIG. 5 in addition to FIGS. 1-3, operations of the addressing unit 50 will now be described. Temporary address sets transmitted from the wireless access node 11 are stored in the memory 51. Only one temporary address set corresponding to a unique MAC address of the first wireless terminal 13 is stored in the memory 51.

[0036] The MAC address filter 53 works together with the memory 51 when a data packet is transmitted from the wireless access node 11 to the first wireless terminal 13. The source address generation unit 55 and the random selection unit 57 work together with memory 51 when a data packet is transmitted from the first wireless terminal 13 to the wireless access node 11. Operations of these components will be described in detail as follows.

[0037] The MAC address filter 53 receives a destination address (DA) extracted from the data packet transmitted from the wireless access node 11, determines whether a temporary address allocated to the destination address (DA) is included in the temporary address set stored in memory 51, and outputs a receipt enable signal indicating receipt of the data packet, according to the determination result. That is, the first wireless terminal 13 receives the data packet sent from the wireless access node 11 when a temporary address allocated to the destination address (DA) is included in the temporary address set stored in memory 51.

[0038] The source address generation unit 55 outputs a random selection signal to the random selection unit 57 when receiving a source address request signal, in order to transmit a data packet from the first wireless terminal 13 to the wireless access node 11. The random selection unit 57 randomly selects a temporary address from the temporary address set stored in memory 51, according to the random selection signal, and outputs the selected temporary address to the source address generation unit 55. The source address generation unit 55 sets the temporary address provided from the random selection unit 57 as the source address (SA), and outputs the source address (SA) to the wireless access node 11.

[0039] That is, whenever data packets are transmitted from the first wireless terminal 13 to the wireless access node 11, each data packet has a different source address from the others. This applies equally to all other wireless terminals in a BSS.

[0040] The above-described preferred embodiments may be embodied as computer programs and may also be embodied on a general-purpose digital computer for executing the computer programs using a computer readable medium. The computer readable medium may include storage media such as magnetic storage media (e.g., ROM's, floppy discs, hard discs, etc.), optically readable media (e.g., CDROMs, DVDs, etc.), and carrier waves (transmissions over the Internet).

[0041] As described above, according to the present invention, it is possible to prevent a MAC address from being exposed during data communication, thereby guaranteeing a user's anonymity, by using a temporary address selected from a temporary address set that contains mappings to a unique MAC address. The temporary address is used as a source address or a destination address upon data communication between a wireless access node and a wireless terminal.

[0042] Also, by using a temporary address randomly selected from a temporary address set, it is possible to prevent the outflow of private information and reduce the risk of attack by malicious users. The temporary address is used as the source address or destination address upon data communication between a wireless access node and a wireless terminal, so that whenever a data packet is transmitted, a different source address or a different destination address is used.

[0043] Preferred embodiments of the present invention have been disclosed herein and, although specific terms are

employed, they are used and are to be interpreted in a generic and descriptive sense only and not for purpose of limitation. Accordingly, it will be understood by those of ordinary skill in the art that various changes in form and details may be made without departing from the scope of the present invention as set forth in the following claims.

Claims

1. A method of guaranteeing users' anonymity in a wireless Local Area Network system, the method comprising:

   creating a plurality of temporary address sets, each of which corresponds to a unique Media Access Control address of a wireless terminal (13), and transmitting each temporary address set to the corresponding wireless terminal (13); and
   performing data packet transmissions between a wireless terminal (13) and a wireless access node (11) using a temporary address selected from the temporary address set corresponding to the wireless terminal (13) as a source address or a destination address.

2. The method as claimed in claim 1, wherein in the creating step, the wireless access node (11) creates the temporary address sets, each of which consists of N, where N is an integer greater than or equal to two, temporary addresses, using a Media Access Control address contained in an access or authentication request message transmitted from a corresponding wireless terminal (13).

3. The method as claimed in claim 1 or 2, wherein in the creating step, the wireless access node (11) encodes the temporary address sets using a predetermined encryption key for each temporary address set, and respectively transmits the encoded temporary address sets to the corresponding wireless terminals (13).

4. The method as claimed in claim 3, wherein each encryption key is created upon authentication of the corresponding wireless terminal (13).

5. The method as claimed in any one of claims 1 to 4, wherein the performing step further comprises:

   a first addressing, which is performed in the wireless access node (11), and generates a temporary address as a destination address randomly selected from the temporary address set corresponding to a wireless terminal (13) that is requesting authentication.

6. The method as claimed in claim 5, wherein the performing step further comprises:

   a second addressing, which is performed in the wireless terminal (13), and generates a temporary address as a source address randomly selected from the temporary address set corresponding to the wireless terminal (13).

7. A computer readable medium having embodied thereon a computer program, comprising program means for performing the steps of the method claimed in any claim of claims 1 through 6.

8. A wireless Local Area Network system for guaranteeing users' anonymity comprising:

   a wireless access node (11) arranged to create a plurality of temporary address sets, each of which corresponds to a unique Media Access Control address of a wireless terminal (13), and use a temporary address selected from each temporary address set as a destination address; and
   at least one wireless terminal (13) arranged to receive a temporary address set corresponding to a unique Media Access Control address thereof from among the plurality of temporary address sets created in the wireless access node (11), and use a temporary address selected from the received temporary address set as a source address.

9. The system as claimed in claim 8, wherein the wireless access (11) node is arranged to create the temporary address sets, each of which consists of N, where N is an integer greater than or equal to two, temporary addresses, using for each address set the MAC address contained in an access or authentication request message transmitted from the corresponding wireless terminal (13).

10. The system as claimed in claim 8 or 9, wherein the wireless access node (11) is arranged to encode the temporary

address sets using a predetermined encryption key for each address set, and respectively transmit the encoded temporary address sets to the corresponding wireless terminals (13).

11. The system as claimed in claim 10, wherein the wireless access node (11) is arranged to create each encryption key upon authentication of the corresponding wireless terminal (13).

12. The system as claimed in any one of claims 8 to 11, wherein the wireless access node (11) comprises:

a first memory (41) for storing the plurality of temporary address sets, each of which consists of N, where N is an integer greater than or equal to two, random addresses, and is created corresponding to a unique Media Access Control address;
a first Media Access Control address filter (43) for filtering a unique MAC address from a source address of a data packet received from a corresponding wireless terminal (13) by referring to the temporary address sets stored in the first memory (41);
a destination address generation unit (45) for enabling a temporary address set corresponding to the unique Media Access Control address of the wireless terminal (13) requesting authentication from among the temporary address sets stored in the first memory (41), for generating a first random selection signal, for generating a temporary address randomly selected from the enabled temporary address set, and for using the temporary address as a destination address; and
a first random selection unit (47) for randomly selecting a temporary address from the temporary address set enabled in the first memory according to the first random selection signal generated in the destination address generation unit (45), and for outputting the selected temporary address to the destination address generation unit (45).

13. The system as claimed in any one of claims 8 to 12, wherein the wireless terminal (13) comprises:

a second memory (51) for receiving a temporary address set from the wireless access node (11) and for storing the temporary address set corresponding to a unique Media Access Control address of the wireless terminal (13);
a second Media Access Control address filter (53) for determining whether a destination address of a data packet received from the wireless access node (11) is included in the temporary address set by referring to the temporary address set stored in the second memory (51), and for generating a receipt enable signal according to a determination result;
a source address generation unit (55) for generating a second random selection signal according to a source address request signal, for generating a temporary address randomly selected from the temporary address set stored in the second memory (51), and for using the temporary address as a source address; and
a second random selection unit (57) for randomly selecting a temporary address from the temporary address set stored in the second memory according to the second random selection signal generated in the source address generation unit (55), and for outputing the selected temporary address to the source address generation unit (55).

Patentansprüche

1. Verfahren zum Garantieren der Anonymität von Benutzern in einem drahtlosen lokalen Netzwerksystem (LAN, local area network), wobei das Verfahren umfasst:

Erstellen einer Mehrzahl von temporären Adressensätzen, deren jeder einer eindeutigen Medienzugangskontrolladresse eines drahtlosen Terminals (13) entspricht und Übertragen jedes temporären Adressensatzes an das entsprechende drahtlose Terminal (13); und
Durchführen von Datenpaketübertragungen zwischen einem drahtlosen Terminal (13) und einem drahtlosen Zugriffsknoten (11) unter Verwendung einer temporären Adresse, die aus dem temporären Adressensatz ausgewählt ist, der dem drahtlosen Terminal (13) entspricht, als Quellenadresse oder als Bestimmungsadresse.

2. Verfahren nach Anspruch 1, worin im Erstellungsschritt der drahtlose Zugriffsknoten (11) temporäre Adressensätze erstellt, deren jeder aus N temporären Adressen besteht, wo N eine ganze Zahl größer oder gleich zwei ist, unter Verwendung einer Medienzugangskontrolladresse, die in einer Zugangs- oder Authentifizierungsanfragemeldung enthalten ist, die von einem entsprechenden drahtlosen Terminal (13) übertragen wird.

3. Verfahren nach Anspruch 1 oder 2, worin im Erstellungsschritt der drahtlose Zugriffsknoten (11) die temporären Adressensätze unter Verwendung eines bestimmten Verschlüsselungsschlüssels für jeden temporären Adressensatz kodiert und entsprechend die kodierten temporären Adressensätze an die entsprechenden drahtlosen Terminals (13) überträgt.

4. Verfahren nach Anspruch 3, worin jeder Verschlüsselungsschlüssel bei Authentifizierung des entsprechenden drahtlosen Terminals (13) erstellt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, worin der Durchführungsschritt ferner umfasst:

eine erste Adressierung, die im drahtlosen Zugriffsknoten (11) durchgeführt wird und eine temporäre Adresse als Bestimmungsadresse erzeugt, die statistisch aus dem temporären Adressensatz ausgewählt wird, der einem drahtlosen Terminal (13) entspricht, das Authentifizierung anfordert.

6. Verfahren nach Anspruch 5, worin der Durchführungsschritt ferner umfasst:

eine zweite Adressierung, die im drahtlosen Terminal (13) durchgeführt wird und eine temporäre Adresse als Quellenadresse erzeugt, die statistisch aus dem temporären Adressensatz ausgewählt wird, der dem drahtlosen Terminal (13) entspricht.

7. Computerlesbares Medium mit einem Computerprogramm darauf verkörpert, das Programmmittel zum Durchführen der Schritte des Verfahrens umfasst, das in einem der Ansprüche 1 bis 6 beansprucht ist.

8. Drahtloses lokales Netzwerksystem (LAN) zum Garantieren der Anonymität von Benutzern, umfassend:

einen drahtlosen Zugriffsknoten (11) so angeordnet, dass er eine Mehrzahl von temporären Adressensätzen erstellt, deren jeder einer eindeutigen Medienzugangskontrolladresse eines drahtlosen Terminals (13) entspricht und Verwenden einer temporären Adresse ausgewählt aus jedem temporären Adressensatz als Bestimmungsadresse; und
mindestens ein drahtloses Terminal (13) so angeordnet, dass es einen temporären Adressensatz entsprechend einer eindeutigen Medienzugangskontrolladresse aus der Mehrzahl von im drahtlosen Zugriffsknoten (11) erstellten temporären Adressen erhält und eine temporäre Adresse ausgewählt aus dem erhaltenen temporären Adressensatz als Quellenadresse verwendet.

9. System nach Anspruch 8, worin der drahtlose Zugriffsknoten (11) so angeordnet ist, dass er die temporären Adressensätze erstellt, deren jeder aus N temporären Adressen besteht, wo N eine ganze Zahl größer oder gleich zwei ist, wobei für jeden Adressensatz die MAC-Adresse verwendet wird, die in einer Zugangs- oder Authentifizierungsanfragemeldung enthalten ist, die vom entsprechenden drahtlosen Terminal (13) übertragen ist.

10. System nach Anspruch 8 oder 9, worin der drahtlose Zugriffsknoten (11) so angeordnet ist, dass er die temporären Adressensätze unter Verwendung eines bestimmten Verschlüsselungsschlüssels für jeden Adressensatz kodiert und entsprechend die kodierten temporären Adressensätze an die entsprechenden drahtlosen Terminals (13) überträgt.

11. System nach Anspruch 10, worin der drahtlose Zugriffsknoten (11) so angeordnet ist, dass er jeden Verschlüsselungsschlüssel bei Authentifizierung des entsprechenden drahtlosen Terminals (13) erstellt.

12. System nach einem der Ansprüche 8 bis 11, worin der drahtlose Zugriffsknoten (11) umfasst:

einen ersten Speicher (41) zum Speichern der Mehrzahl von temporären Adressensätzen, deren jeder aus N statistischen Adressen besteht, wo N eine ganze Zahl größer oder gleich zwei ist und entsprechend einer eindeutigen Medienzugangskontrolladresse erstellt ist;
einen ersten Medienzugangskontrolladressenfilter (43) zum Filtern einer eindeutigen MAC-Adresse aus einer Quellenadresse eines Datenpakets, das von einem entsprechenden drahtlosen Terminal (13) empfangen ist, durch Bezugnahme auf die temporären Adressensätze, die im ersten Speicher (41) gespeichert sind;
eine Bestimmungsadressenerzeugungseinheit (45) zur Freigabe eines temporären Adressensatzes entsprechend der eindeutigen Medienzugangskontrolladresse des drahtlosen Terminals (13), das Authentifizierung anfordert, unter den temporären Adressensätzen, die im ersten Speicher (41) gespeichert sind, zum Erzeugen

eines ersten statistischen Auswahlsignals zum Erzeugen einer temporären Adresse, die statistisch aus dem freigegebenen temporären Adressensatz ausgewählt ist, und zum Verwenden der temporären Adresse als Bestimmungsadresse; und
eine erste statistische Auswahleinheit (47) zum statistischen Auswählen einer temporären Adresse aus dem temporären Adressensatz, der im ersten Speicher freigegeben ist, gemäß dem ersten statistischen Auswahlsignal, das in der Bestimmungsadressenerzeugungseinheit (45) erzeugt ist, und zum Ausgeben der ausgewählten temporären Adresse an die Bestimmungsadressenerzeugungseinheit (45).

13. System nach einem der Ansprüche 8 bis 12, worin das drahtlose Terminal (13) umfasst:

einen zweiten Speicher (51) zum Empfangen eines temporären Adressensatzes vom drahtlosen Zugriffsknoten (11) und zum Speichern des temporären Adressensatzes entsprechend einer eindeutigen Medienzugangskontrolladresse des drahtlosen Terminals (13);
einen zweiten Medienzugangskontrolladressenfilter (53) zum Bestimmen, ob eine Bestimmungsadresse eines vom drahtlosen Zugriffsknoten (11) empfangenen Datenpaktes im temporären Adressensatz enthalten ist, durch Bezugnahme auf den temporären Adressensatz, der im zweiten Speicher (51) gespeichert ist, und zum Erzeugen eines Empfangsfreigabesignals entsprechend einem Bestimmungsergebnis;
eine Quellenadressenerzeugungseinheit (55) zum Erzeugen eines zweiten statistischen Auswahlsignals entsprechend einem Quellenadressenanfragesignal zum Erzeugen einer temporären Adresse, die aus dem temporären Adressensatz statistisch ausgewählt ist, der im zweiten Speicher (51) gespeichert ist, und zum Verwenden der temporären Adresse als Quellenadresse; und
eine zweite statistische Auswahleinheit (57) zum statistischen Auswählen einer temporären Adresse aus dem temporären Adressensatz, der im zweiten Speicher gespeichert ist, entsprechend dem zweiten statistischen Auswahlsignal, das in der Quellenadressenerzeugungseinheit (55) erzeugt ist, und zum Ausgeben der ausgewählten temporären Adresse an die Quellenadressenerzeugungseinheit (55).

Revendications

1. Procédé pour garantir l'anonymat des utilisateurs dans un système de réseau local sans fil, le procédé comprenant :

la création d'une pluralité d'ensembles d'adresses provisoires, chacun d'eux correspondant à une adresse unique de contrôle d'accès au support (MAC) d'un terminal sans fil (13), et la transmission de chaque ensemble d'adresses provisoires au terminal sans fil correspondant (13) ; et
l'exécution de transmissions de paquets de données entre un terminal sans fil (13) et un noeud d'accès sans fil (11) en utilisant une adresse provisoire sélectionnée dans l'ensemble d'adresses provisoires correspondant au terminal sans fil (13) comme adresse d'origine ou adresse de destination.

2. Procédé selon la revendication 1, dans lequel, dans l'étape de création, le noeud d'accès sans fil (11) crée les ensembles d'adresses provisoires, chacun d'eux se composant de N adresses provisoires, où N est un nombre entier supérieur ou égal à deux, en utilisant une adresse de contrôle d'accès au support contenue dans un message de demande d'accès ou d'authentification transmis à partir d'un terminal sans fil correspondant (13).

3. Procédé selon l'une quelconque des revendications 1 ou 2, dans lequel dans l'étape de création, le noeud d'accès sans fil (11) code les ensembles d'adresses provisoires en utilisant une clé de chiffrement prédéterminée pour chaque ensemble d'adresses provisoires, et transmet respectivement les ensembles d'adresses provisoires codés, aux terminaux sans fil correspondants (13).

4. Procédé selon la revendication 3, dans lequel chaque clé de chiffrement est créée lors de l'authentification du terminal sans fil correspondant (13).

5. Procédé selon l'une quelconque des revendications 1 à 4, dans lequel l'étape d'exécution comprend de plus : un premier adressage qui est exécuté dans le noeud d'accès sans fil (11), et génère une adresse provisoire en tant qu'adresse de destination sélectionnée aléatoirement dans l'ensemble d'adresses provisoires correspondant à un terminal sans fil (13) qui demande une authentification.

6. Procédé selon la revendication 5, dans lequel l'étape d'exécution comprend de plus : un deuxième adressage qui est exécuté dans le terminal sans fil (13), et génère une adresse provisoire en tant qu'adresse d'origine sélectionnée

aléatoirement dans l'ensemble d'adresses provisoires correspondant au terminal sans fil (13).

7. Support pouvant être lu par un ordinateur dans lequel est incorporé un programme d'ordinateur comprenant des moyens formant programme, pour exécuter les étapes du procédé revendiqué dans l'une quelconque des revendications 1 à 6.

8. Système de réseau local sans fil pour garantir l'anonymat des utilisateurs, comprenant :

un noeud d'accès sans fil (11) agencé afin de créer une pluralité d'ensembles d'adresses provisoires, chacun d'eux correspondant à une adresse unique de contrôle d'accès au support d'un terminal sans fil (13), et pour utiliser une adresse provisoire sélectionnée dans chaque ensemble d'adresses provisoires en tant qu'adresse de destination ; et
au moins un terminal sans fil (13) agencé pour recevoir un ensemble d'adresses provisoires correspondant à une adresse unique de contrôle d'accès au support de celui-ci, parmi la pluralité d'ensembles d'adresses provisoires créés dans le noeud d'accès sans fil (11), et pour utiliser une adresse provisoire sélectionnée dans l'ensemble d'adresses provisoires reçu, en tant qu'adresse d'origine.

9. Système selon la revendication 8, dans lequel le noeud d'accès sans fil (11) est agencé pour créer les ensembles d'adresses provisoires, chacun d'eux se composant de N adresses provisoires, où N est un nombre entier supérieur ou égal à deux, en utilisant pour chaque ensemble d'adresses, l'adresse MAC contenue dans un message de demande d'accès ou d'authentification transmis à partir d'un terminal sans fil correspondant (13).

10. Système selon l'une quelconque des revendications 8 ou 9, dans lequel le noeud d'accès sans fil (11) est agencé pour coder les ensembles d'adresses provisoires en utilisant une clé de chiffrement prédéterminée pour chaque ensemble d'adresses, et pour transmettre respectivement les ensembles d'adresses provisoires codés, aux terminaux sans fil correspondants (13).

11. Système selon la revendication 10, dans lequel le noeud d'accès sans fil (11) est agencé pour créer chaque clé de chiffrement lors de l'authentification du terminal sans fil correspondant (13).

12. Système selon l'une quelconque des revendications 8 à 11, dans lequel le noeud d'accès sans fil (11) comprend :

une première mémoire (41) pour stocker la pluralité d'ensembles d'adresses provisoires, chacun d'eux se composant de N adresses aléatoires, où N est un nombre entier supérieur ou égal à deux, et étant créé correspondant à une adresse unique de contrôle d'accès au support ;
un premier filtre d'adresse de contrôle d'accès au support (43) pour filtrer une adresse unique MAC à partir d'une adresse d'origine d'un paquet de données reçu en provenance d'un terminal sans fil correspondant (13) en se référant aux ensembles d'adresses provisoires stockés dans la première mémoire (41) ;
une unité de génération d'adresse de destination (45) pour valider un ensemble d'adresses provisoires correspondant à l'adresse unique de contrôle d'accès au support du terminal sans fil (13) qui demande une authentification parmi les ensembles d'adresses provisoires stockés dans la première mémoire (41), pour générer un premier signal de sélection aléatoire, pour générer une adresse provisoire sélectionnée aléatoirement dans l'ensemble d'adresses provisoires validé, et pour utiliser l'adresse provisoire en tant qu'adresse de destination ; et
une première unité de sélection aléatoire (47) pour sélectionner aléatoirement une adresse provisoire dans l'ensemble d'adresses provisoires validé dans la première mémoire selon le premier signal de sélection aléatoire généré dans l'unité de génération d'adresse de destination (45), et pour délivrer en sortie l'adresse provisoire sélectionnée, à l'unité de génération d'adresse de destination (45).

13. Système selon l'une quelconque des revendications 8 à 12, dans lequel le terminal sans fil (13) comprend :

une deuxième mémoire (51) pour recevoir un ensemble d'adresses provisoires en provenance du noeud d'accès sans fil (11) et pour stocker l'ensemble d'adresses provisoires correspondant à une adresse unique de contrôle d'accès au support du terminal sans fil (13) ;
un deuxième filtre d'adresse de contrôle d'accès au support (53) pour déterminer si une adresse de destination d'un paquet de données reçu en provenance du noeud d'accès sans fil (11), est incluse dans l'ensemble d'adresses provisoires en se référant à l'ensemble d'adresses provisoires stocké dans la deuxième mémoire (51), et pour générer un signal de validation de réception selon le résultat de la détermination ;

une unité de génération d'adresse d'origine (55) pour générer un deuxième signal de sélection aléatoire selon un signal de demande d'adresse d'origine, pour générer une adresse provisoire sélectionnée aléatoirement dans l'ensemble d'adresses provisoires stocké dans la deuxième mémoire (51), et pour utiliser l'adresse provisoire en tant qu'adresse d'origine ; et

une deuxième unité de sélection aléatoire (57) pour sélectionner aléatoirement une adresse provisoire dans l'ensemble d'adresses provisoires stocké dans la deuxième mémoire selon le deuxième signal de sélection aléatoire généré dans l'unité de génération d'adresse d'origine (55), et pour délivrer en sortie l'adresse provisoire sélectionnée, à l'unité de génération d'adresse d'origine (55).

FIG. 1

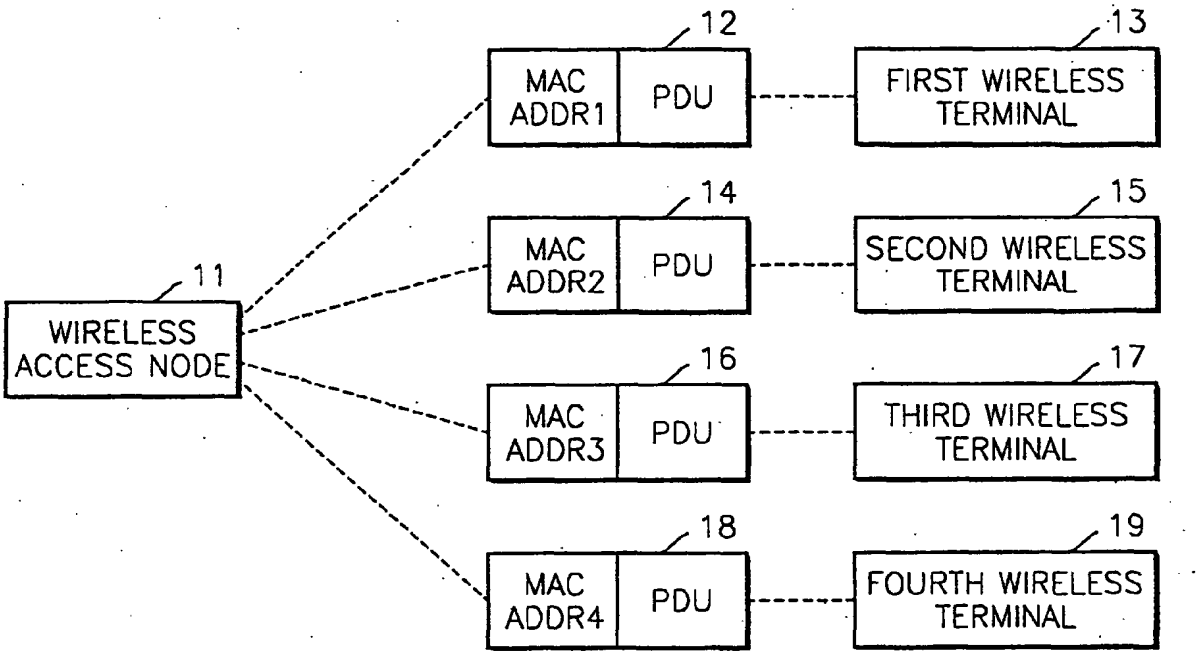

11
WIRELESS ACCESS NODE
12
MAC ADDR1
PDU
13
FIRST WIRELESS TERMINAL
14
MAC ADDR2
PDU
15
SECOND WIRELESS TERMINAL
16
MAC ADDR3
PDU
17
THIRD WIRELESS TERMINAL
18
MAC ADDR4
PDU
19
FOURTH WIRELESS TERMINAL

FIG. 2

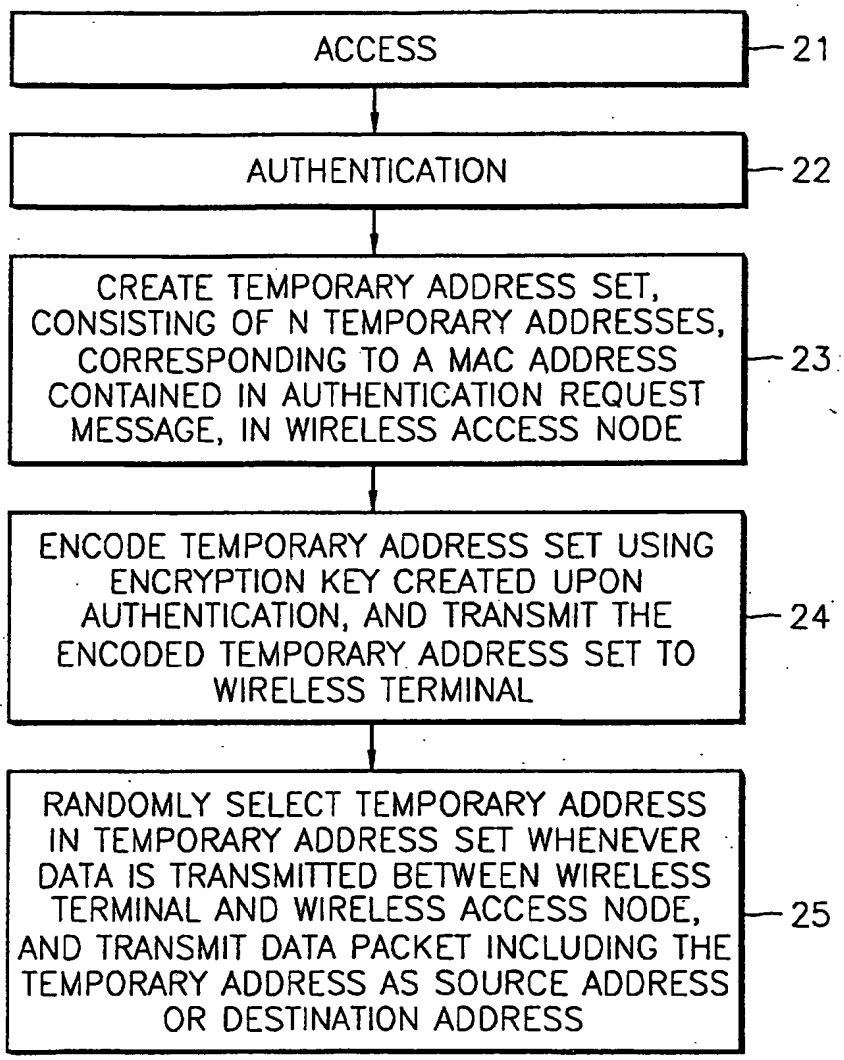

ACCESS
21
AUTHENTICATION
22
CREATE TEMPORARY ADDRESS SET, CONSISTING OF N TEMPORARY ADDRESSES, CORRESPONDING TO A MAC ADDRESS CONTAINED IN AUTHENTICATION REQUEST MESSAGE, IN WIRELESS ACCESS NODE
23
ENCODE TEMPORARY ADDRESS SET USING ENCRYPTION KEY CREATED UPON AUTHENTICATION, AND TRANSMIT THE ENCODED TEMPORARY ADDRESS SET TO WIRELESS TERMINAL
24
RANDOMLY SELECT TEMPORARY ADDRESS IN TEMPORARY ADDRESS SET WHENEVER DATA IS TRANSMITTED BETWEEN WIRELESS TERMINAL AND WIRELESS ACCESS NODE, AND TRANSMIT DATA PACKET INCLUDING THE TEMPORARY ADDRESS AS SOURCE ADDRESS OR DESTINATION ADDRESS
25

FIG. 3

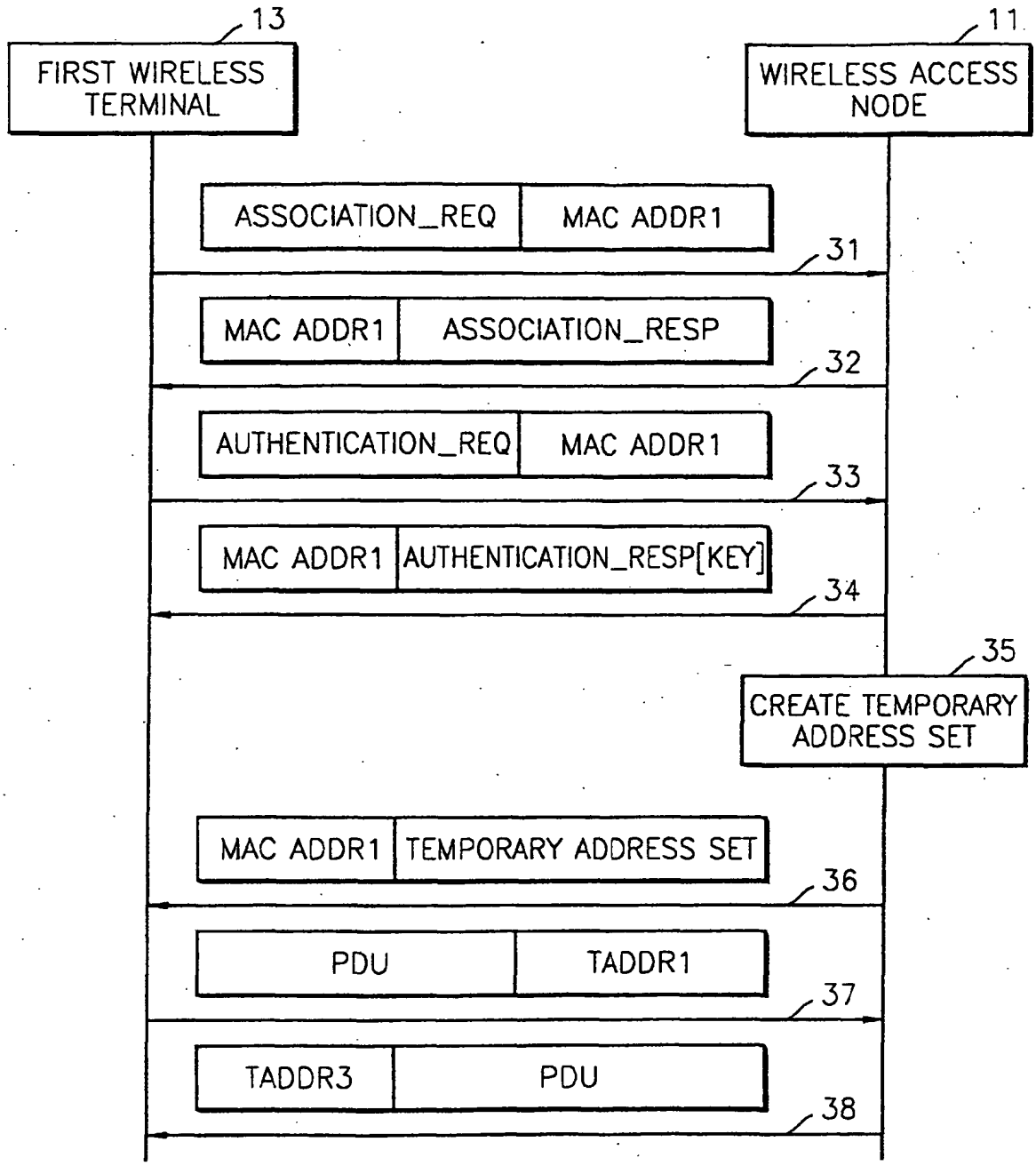

13
FIRST WIRELESS TERMINAL
11
WIRELESS ACCESS NODE
ASSOCIATION_REQ
MAC ADDR1
31
MAC ADDR1
ASSOCIATION_RESP
32
AUTHENTICATION_REQ
MAC ADDR1
33
MAC ADDR1
AUTHENTICATION_RESP[KEY]
34
35
CREATE TEMPORARY ADDRESS SET
MAC ADDR1
TEMPORARY ADDRESS SET
36
PDU
TADDR1
37
TADDR3
PDU
38

FIG. 4

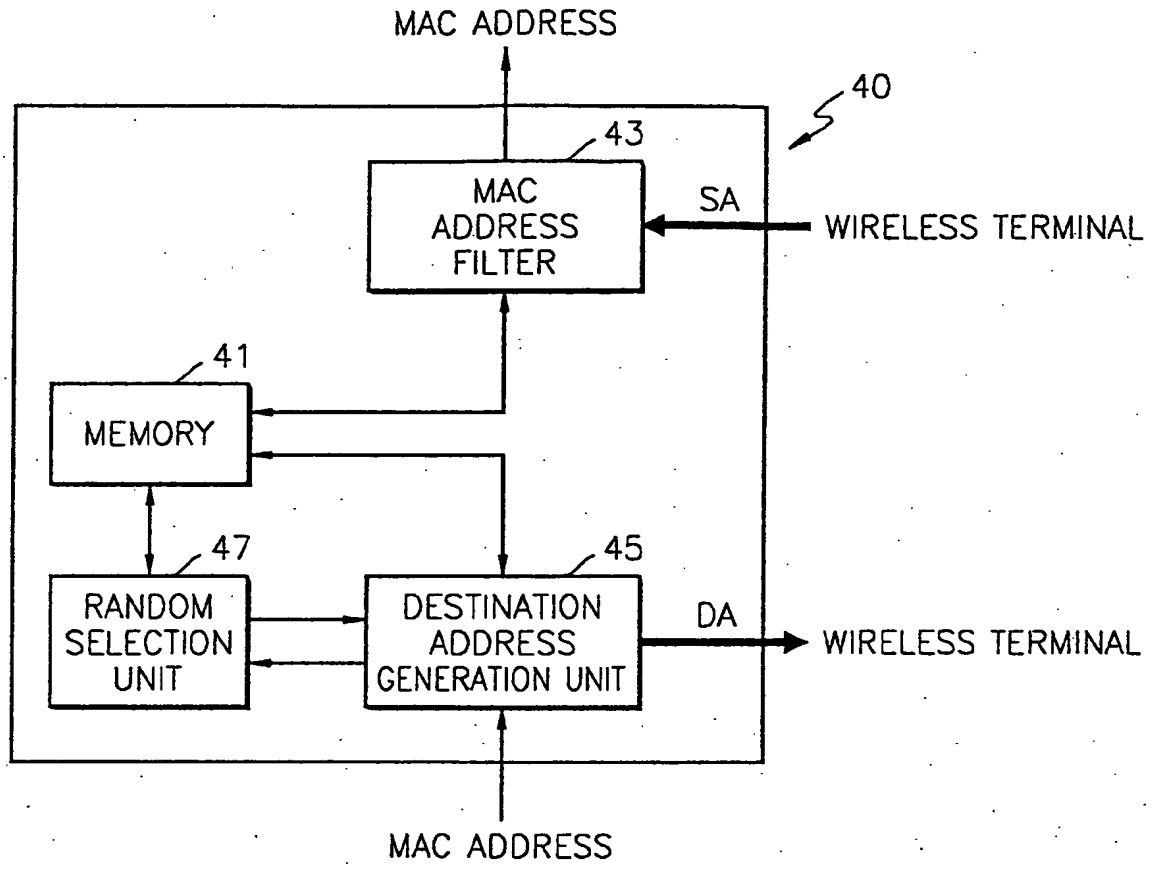
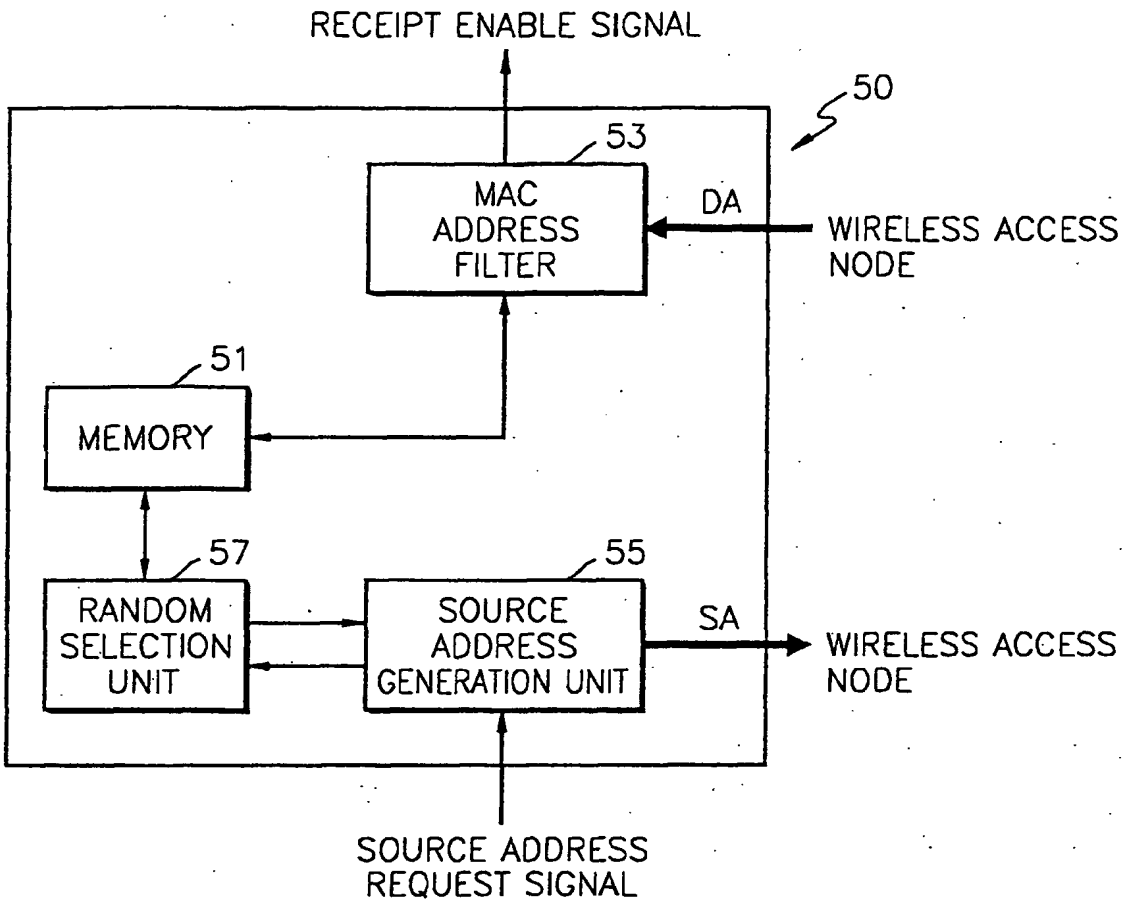

MAC ADDRESS
40
43
MAC ADDRESS FILTER
SA
WIRELESS TERMINAL
41
MEMORY
47
RANDOM SELECTION UNIT
45
DESTINATION ADDRESS GENERATION UNIT
DA
WIRELESS TERMINAL
MAC ADDRESS

FIG. 5


RECEIPT ENABLE SIGNAL
50
53
MAC ADDRESS FILTER
DA
WIRELESS ACCESS NODE
51
MEMORY
57
RANDOM SELECTION UNIT
55
SOURCE ADDRESS GENERATION UNIT
SA
WIRELESS ACCESS NODE
SOURCE ADDRESS REQUEST SIGNAL